年金個人情報に関する情報セキュリティ対策の実施状況及び年金個人情報の流出が日本年金機構の業務に及ぼした影響等について

1　検査の背景

(1) 日本年金機構における個人情報、情報システム及び情報セキュリティ対策の概要

厚生労働省及び日本年金機構は、厚生年金保険等の被保険者等の基礎年金番号、氏名、保険料の納付状況等の個人情報(年金個人情報)について、社会保険オンラインシステム、機構LANシステム等で構成されている年金情報システムにより管理することとしている。

そして、同省及び機構は、年金個人情報がプライバシー性の非常に高い情報であることなどから、年金個人情報等に関する情報セキュリティを確保するための対策等に関する規程である情報セキュリティポリシー(「厚労省ポリシー」及び「機構ポリシー」)を定めている。

また、機構は、インターネットに接続されている機構LANシステム上の共有フォルダに年金個人情報を保存することは、原則として禁止しているが、所要のアクセス制限やパスワードの設定を行うことを前提に、これを例外的に認めている。

(2) 年金個人情報の流出とその検証の概要

機構は、平成27年5月、外部から標的型攻撃(注1)を受けて、その結果、機構LANシステム上の共有フォルダに保存されていた125万件の基礎年金番号、氏名等の年金個人情報がインターネットを通じて不正に外部に流出したとしている(この標的型攻撃による年金個人情報の流出を「流出事案」)。

流出事案の事実関係等が取りまとめられた検証報告書等によれば、流出事案を発生させた直接的な要因は、機構において、標的型攻撃を受けた場合における対応については、LANケーブルの抜線以外に具体的な定めがなく、不正なプログラムの感染の有無等の事態の確認が遅れ、有効な対策が講じられなかったことであるとされている。

(注1)　標的型攻撃　　不正なプログラムを含むファイルを添付するなどしたメールを職員に対して送りつけ、添付ファイルを開封するなどした職員の端末を介してネットワークに不正に侵入するなどのサイバー攻撃

(3) 流出事案の再発防止に向けた取組の概要

同省は、流出事案の再発を防止するために、「情報セキュリティ強化等に向けた組織・業務改革」を27年9月18日に公表している。

一方、機構は、日本年金機構法第49条第1項の規定に基づく厚生労働大臣の業務改善命令を受けて、業務改善計画を策定して27年12月9日に厚生労働大臣に提出しており、再発防止に向けて機構が既に執った対策及び今後実施する取組を明らかにするなどしている。

(4) 流出事案が機構の業務に及ぼした影響の概要

機構は、年金個人情報が流出した者(年金個人情報流出者)に対して、年金個人情報の流出に対するおわびを記した文書(おわび文書)、基礎年金番号の変更を通知する文書(基礎年金番号変更通知)等を送付している。そして、これらの対応に必要な経費としては10億円が見込まれるとしている。

また、機構は、流出事案発生以前には、国民年金保険料の未納者に対して納付督励業務を行っており、納付督励業務には、機構が自ら実施する業務(機構納付督励業務)と、機構から委託を受けた民間事業者が実施する業務(市場化納付督励業務)とがある。

しかし、流出事案の発生を踏まえ、機構は、27年6月に通知を発し、一定期間、納付督励業務の一部を行わないこととしていた。

2　検査の着眼点

本院は、流出事案の発生前において、機構における年金個人情報に関する情報セキュリティ対策は適切に行われていたか、同省及び機構におけるその実効性を確保するための監査等は適切に

行われていたか、また、流出事案の発生後において、機構の年金個人情報に関する情報セキュリティ対策及び流出事案への対応業務は適切に行われているか、流出事案の発生は機構の業務にどのような影響を及ぼしているか、その後の同省及び機構における再発防止に向けた取組の進捗状況はどのようになっているかなどに着眼して検査した。

3　検査の状況

(1) 流出事案の発生前における年金個人情報に関する情報セキュリティ対策等の実施状況及び流出事案発生後における年金個人情報の保存等の状況

ア　流出事案の発生前における機構ポリシーの改正の状況についてみたところ、厚労省ポリシーの改正から一定の期間、統合ネットワーク内でセキュリティ水準の異なる期間が生ずるなどしてしまうのに、機構において厚労省ポリシーの改正後速やかに機構ポリシーの改正を行っておらず、また同省及び機構において、機構ポリシーの改正に向けた連携等が十分であったとは認め難い状況となっていた。

イ　流出事案の発生前における同省の機構に対する監査及び機構の内部監査の実施状況についてみたところ、機構ではインシデント(注2)対処手順書を策定していないなどしていたのに、いずれの監査においても、情報セキュリティに関する体制整備が十分でないことについて指摘したことはない状況となっていた。

また、機構の監査部は、所要のアクセス制限等の設定が行われないまま年金個人情報が共有フォルダに保存されていることを把握し、機構の担当部署に対して改善要請を発していたが、この改善要請は内部監査の結果ではないなどとして機構の理事長に対して報告しておらず、また、実際の改善状況等に対する監査等を実施していなかった。そして、機構において、監査部の改善要請への対応は徹底されていなかったと認められた。

(注2)　インシデント　コンピュータシステムにおけるセキュリティの確保に脅威を及ぼす事象又はその可能性のある事象

ウ　流出事案の発生前における同省の機構に対する情報セキュリティに関する指導等の状況についてみたところ、同省年金局は、機構に対して、所要の注意喚起等を十分に行っていなかった。

エ　流出事案発生後の機構における年金個人情報の保存状況等についてみたところ、専用PCのハードディスクに年金個人情報が保存されていることが確認された。

そこで、本院は、機構に対して、専用PCのハードディスクに保存されている年金個人情報の有無等について報告を求めた。これに対して、機構は、機構本部及び全国の年金事務所等の専用PCのハードディスクに保存されていた年金個人情報については、28年8月から同年9月までの間に、専用フォルダに移し替えるなどした上で全て削除したと本院に報告した。

その後、28年10月及び同年11月の会計実地検査において、上記のとおり、機構は、年金個人情報については専用フォルダに移し替えるなどした上で全て削除したとしていたのに、専用PCのハードディスクに年金個人情報等が保存されていることが確認された。

(2) 流出事案の対応に要する経費の支出、対応業務等の状況

ア　機構の流出事案の発生に対応するための経費として見込んだ額10億円の支出額は、27年度決算額で10億8379万円となっており、これらの経費は、年金個人情報流出者に対する問合せ対応等に要する経費に限定されていた。上記のほかに、共有フォルダに保存されている電子ファイル内に年金個人情報が存在しているかどうかを調査するための経費等が見受けられた。また、同省でも、流出事案が発生したことにより支出されたと考えられる経費があり、これらの経費を合算すると計9418万円(同省分4687万円、機構分4730万円)となる。

また、機構が流出事案の発生に対応する経費に充てるためにねん出したとしている財源の中には、27年度には支出されないものの、28年度以降において支出する必要があるものが含まれていると認められた。

イ　おわび文書又は基礎年金番号変更通知等が返送された年金受給者計6,988人に対する年金支給の状況についてみたところ、年金受給者の所在が確認できないのに、機構は、これらの者の生存等の事実について更に確認しないまま年金支給を継続していた。機構においては、年金受給者の所在が確認できないという情報を有効に活用し、その生存等の事実を確認することなどについて検討する必要があったと認められる。

(3) 流出事案の発生により中止した業務の影響等

ア　機構は、流出事案の発生に対応するため、機構納付督励業務の一部を27年6月から5か月の間行っていなかった。

そこで、上記5か月の間に督促状等を送付しなかったことにより消滅時効期間が経過した国民年金保険料の債権額等について本院において試算すると、8,159か月分、1億2115万円となり、このうち、仮に流出事案の影響なく督促状を送付できていれば、消滅時効が中断され、消滅時効期間の経過前に納付されたと考えられる国民年金保険料の債権額等について試算すると3,769か月分、5659万円となる。

また、5か月の間に特別催告状の送付をしなかったことを踏まえ、当初の行動計画等のとおりに特別催告状を送付した場合に収納が見込まれる国民年金保険料の額等について試算すると、計759,967か月分、計118億4788万円となる。

イ　機構は、27年6月に電話による問合せに対する対応以外の市場化納付督励業務を行わないよう民間事業者に対して求めていて(市場化納付督励業務を行わないこととされた期間を「業務委託中止期間」)、業務委託中止期間はその後5か月に及んでいる。そこで、委託費の支払についてみたところ、機構は、業務委託中止期間を含む27年5月から28年4月までの1年間に係る委託費として計66億2112万円を12等分して毎月支払っていた。なお、機構は、民間事業者が業務委託中止期間中に業務を実施しなかったことによる27年度の実績の減少も踏まえて精算を行うなどとして、28年10月に、民間事業者6社のうち5社に対して、27年度分の支払済みの委託費計2億3122万円の返還を求めている。

(4) 再発防止の取組の進捗状況

27年9月に「情報セキュリティ強化等に向けた組織・業務改革」が公表されてから28年9月までの間における同省の再発防止の取組の進捗状況についてみたところ、統合ネットワーク等において高度な標的型攻撃に対応するためのシステム改修等を行うなどしていた。

また、27年12月に業務改善計画が提出されてから28年9月までの間における機構の再発防止の取組の進捗状況についてみたところ、年金個人情報の管理・運用を行う領域をインターネットから完全に分離した年金情報システムの構築に向けた取組を進めるなどしていた。

4　所見

同省及び機構において、本院の検査により明らかとなった状況等を踏まえ、次のような点に留意して、年金個人情報の管理に関する一層の体制の整備を図るなどの必要があると認められる。

ア　機構において、厚労省ポリシーが改正された場合には、その改正内容に準拠して機構ポリシーを速やかに改正するなどするとともに、同省と機構との適切な連携等を図るなどして、年金個人情報に関する情報セキュリティ対策を適切に行うこと

イ　同省及び機構において、年金個人情報に関する情報セキュリティ監査を含め、同省の機構に対する監査及び機構の内部監査を一層実効性のあるものとすること

ウ　機構において、年金支給を適切に行うために、おわび文書等が返送されていて年金受給者の所在が確認できないという情報を有効に活用し、その生存等の事実を確認することなどについて検討すること

エ　機構において、機構が策定した業務改善計画に記載されている再発防止の取組を一層着実に実施すること

同省及び機構は、年金に関する業務の実施に当たり、今後とも膨大な年金個人情報を長期にわたり保有し、取り扱うことが見込まれる。本院は、これらを踏まえて、機構において情報セキュリティ対策が適切に実施されているか、同省及び機構において実効性のある監査等が行われているか、また、流出事案の影響等を踏まえた適切な対応が行われているか、さらに、機構の再発防止の取組が着実に行われているかなどについて、引き続き検査していくこととする。